



08/416037
895493

58700.919

UNITED STATES PATENT APPLICATION

FOR

METHOD FOR CONTROLLING DATABASE COPYRIGHTS

INVENTORS:

SHUNICHI MOMIKI
MAKOTO SAITO

I hereby certify that this correspondence is being
deposited with the United States Postal Service
as Express Mail (Label No. 782564052045) in
an envelope addressed to: Commissioner of Patents
and Trademarks, Washington, D.C. 20001

on: March 31, 1995
(Date of Deposit)
Emily Ruzicka 3/31/95
(Signature) Req. No. (Date)

PREPARED BY:

HECKER & HARRIMAN
2029 Century Park East
Suite 1600
Los Angeles, CA 90067

(310) 286-0377



A *W* *Lee*
08/416037
895493

BACKGROUND OF THE INVENTION

Ans
(B)
1. FIELD OF THE INVENTION

5 The present invention relates to a method for controlling copyrights on utilizing, storing, copying, editing and transferring of digital data, and in particular, to an application of the method to a multimedia system.

2. BACKGROUND ART

10

In the information oriented society of today, database systems are becoming wide spread in which it is possible to use various types of data, stored independently by each computer in the past, by connecting computers via communication lines.

15

In such a database system, the information handled up to this point has been conventionally coded information that can be processed by computer, and that contains a relatively small amount of information and monochrome binary data, such as facsimile information at the most. It is not possible to handle data containing a relatively large amount of information, such as data for natural pictures or animation.

25 With the rapid progress of digital processing techniques for various types of electrical signals, a technique is under development for digital processing of picture signals other than binary data, handled only as analog signals in the past.

30 By digitizing the picture signal, it is possible to handle a picture signal, such as television signal, by computer. As a technique of the future, attention is now focused on "multimedia systems", which can simultaneously handle the data processed by computers and digitized picture data. Because the

picture data contains an overwhelmingly large amount of information compared with character data and audio data, it is difficult to store, transfer or process the picture data by computer. For this reason, techniques for compressing and expanding picture data have been developed. Further, several standards for compression/expansion of picture data have been established. For example, the following standards have been established as common standards: JPEG (Joint Photographic image coding Experts Group) standards for still pictures, H.261 standards for television conferences, MPEG1 (Moving Picture image coding Experts Group 1) standards for picture accumulation, and MPEG2 standards to cope with current television broadcasting and high definition television broadcasting. By implementing these new techniques, it is now possible to transmit digital picture data in real time.

For analog data, which has been widely used in the past, the control of copyrights during processing has not been an important issue because the quality of the analog data deteriorates each time the data is stored, copied, edited or transferred. However, the quality of digital data does not deteriorate even when the data is repeatedly stored, copied, ^{edited} ~~fabricated~~ or transferred. Therefore, the management and control of copyrights during processing of digital data is an important issue.

Up to now, there has been no adequate method for management and control of copyrights for digital data. It has been managed and controlled merely by copyright law or by contracts. In copyright law, only compensation for digital sound and picture recording devices has been prescribed.

It is possible not only to refer to the content of a database, but also to effectively utilize the data obtained from the database by storing, copying or editing the data, and also transferring the edited data to other persons or to the database with the edited data registered as new data.

In a conventional database system, only character data is handled.
a However, in multimedia systems, sound data and picture data, originally
generated as analog data, is digitized and used as part of the database in
5 addition to the other data in the database, such as character data.

Under such circumstances, it is an important question as to how to
handle copyrights of the data in the database. However, there are no means
in the prior art for copyright management and control of such actions as
10 copying, editing, transferring, etc., of data.

A system for executing copyright control by using encrypted data and
obtaining a permit key from a key control center via public telephone lines is
disclosed in Japanese Patent Application 4-199942 (US-08/098415) and
15 Japanese Patent Application 4-289074 (US-08/143912) of the present inventors.
A device for this purpose is disclosed in Japanese Patent Application 4-276941
(US-08/135634), also of the present inventors.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide a method for controlling copyrights in the display (including the process of providing
5 sound), storage, copying, editing and transfer of digital data in a database system including real time transmission of digital pictures.

a
For the control of copyrights in the database system to which the present invention is applied, it is essential to transmit one or more ~~copyright~~
10 ~~control messages with copyright information~~ and a program for controlling copyrights, when necessary, in addition to a key for enabling users who wish to use encrypted data.

The copyright control message is displayed on a screen and advises or
15 warns the user if the data is being utilized in a manner inconsistent with the conditions of the user's request or permission. The copyright control program watches and controls data use so that the data is not utilized beyond the conditions of the user's request or permission.

20 The copyright control program, the copyright information and the copyright control message are supplied together with a permit key in some cases, but they may also be supplied together with data in other cases. It is also possible to supply a part of them together with the permit key, and to supply the other part with the data.

25

For the data, the permit key, the copyright control message, the copyright information and the copyright control program, there are the following three cases: they are transmitted in encrypted form and decrypted upon use; they are transmitted in encrypted form and decrypted only when
30 they are displayed; or they are not encrypted at all.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1A and Fig. 1B illustrate examples of display messages of the present invention.

5

Fig. 2A and Fig. 2B illustrate structures for television signals.

Sup A2

Fig. 3A to Fig. 3J illustrate embodiments of the present invention.

Sup A2
Sup A3

DETAILED DESCRIPTION

In the following, description will be given on embodiments of the present invention.

5

Sub D₀

In the prior patent applications mentioned above, it is assumed that a permit key obtaining route is different from a data obtaining route as shown in Fig. 3A, and that the permit key is obtained from a key control center via public telephone lines. However, if a charging method is determined, it is possible to obtain the permit key via the communication system through which the database is supplied.

Sub D₂

In the system of the prior patent applications, it is assumed that the permit key for secondary exploitation is used for distribution of the data selected for secondary exploitation. Secondary exploitation involving the storing, copying, editing, transferring, etc. of data is not included in the assumption. Also, it is assumed that the data is distributed only inside a LAN to which the users belong. Distribution outside the LAN is not part of the assumption. Therefore, the system is not adequate to cope with secondary exploitation unless the users choose to honor the copyright.

0

Imp.
A₀
D₃

To cope with various forms of the secondary exploitation as described above, ^{in the present invention} a plurality of permit keys are prepared to match each form of use, and no utilization is possible unless there is a permit key suitable for the desired form of use. As to the forms of use available for a database, there are display, storage, copying, edit, transfer, etc. The permit keys suitable for these forms of use should be prepared. However, in the case where the ability to execute several forms of use at the same time is desired, it is necessary to obtain a plurality of permit keys. If the user fails to obtain the permit keys, the desired form of use may not be executed.

To avoid such situations, a permit key can be used which makes it possible to execute several forms of use. Hierarchical permit keys can be used such that an upper level key also fulfills the function of a lower level key. For example, from lower level to upper level, the hierarchy is defined as:

5 display < storage < copying < edit < transfer. With the display permit key, only display operations can be executed. Display and storage operations can be executed by the storage permit key. Display, storage and copying operations can be executed by the copying permit key. Display, storage, copying and edit operations can be executed by the edit permit key. Display, storage, copying,

10 edit and transfer operations can be executed by the transfer permit key.

In the prior patent application, i.e. Japanese Patent Application 4-276941 (US-08/135634), the present inventors have proposed a system in which a plurality of encrypted data files, each encrypted by ^{one of} a plurality of different ^{crypt} encryption keys, are recorded (stored) in encrypted form. The data files ^{are} ^{is} then decrypted ^{it is utilized} when they are displayed or edited, for instance, in a system where the storage permit key is the lowest level key.

^{On the relation of keys}

By applying this system, it is possible to order key hierarchy from

20 lower-level to upper-level in the order of: storage < copying < transfer < display < edit. Specifically, the order is set in such manner that storage operations can be executed by a storage permit key; storage and copying operations can be executed by a copying permit key; storage, copying and transfer operations can be executed by a transfer permit key; storage, copying,

25 transfer and display operations can be executed by a display permit key; and storage, copying, transfer, display and edit operations can be executed by an edit permit key.

In this system, storage, copying and transfer are placed at a lower level

30 than display because, even when storage, copying and transfer operations are executed on the data, it is difficult and meaningless to utilize the data since it

0 a cannot be displayed. It is necessary to ^{display the data} ~~execute display~~ in order to utilize the data. This hierarchical arrangement is best suited to a system, in which encrypted data are supplied and are utilized using a permit key.

5 The permit key is usually offered to the user on payment basis.
Therefore, except where data utilization is unlimited, the number of times
D the permit key may be used is limited to one time or several times ~~if it is~~
D ~~necessary to limit the number of times the data is used.~~

10 Because the data can be used if there is a permit key, it is possible to use the data beyond the permitted range if the permit key is duplicated or falsified. To prevent this, the permit key is encrypted.

Sub D₄ The use of data includes storage, display, copying, edit, transfer, etc.

15 thereof, which are necessary to be allowed or prohibited.

In the case where it is necessary to limit the number of usage times or to limit forms of use, it is desirable to display a message for such purpose.

20 In the case where the information under copyright is falsified, the data supplier or the user may suffer damages. This must be prevented.

D
To ensure complete copyright control, information on the original copyright and information on secondary and tertiary copyrights for the
25 edition of the data are given to the data.

The above copyright control is executed by the copyright control program.

30 In a conventional database system, the data itself is offered in a completely defenseless state. Therefore, copyright control can be executed

only when data is taken out of the database. In the subsequent copyright control, there is no other way but to rely on ^{the} conscience of the user and to take necessary measures when the data is utilized beyond the permitted range of use.

5
In: A2
D For this reason, ^{in an embodiment of the invention} as described in the prior patent application, i.e.

D Japanese Patent Application 4-276941 (US 08/135634), the data supplied from
D the database ^{is left} are left in an encrypted state, and storage is executed under this condition. In addition, copying and transfer are also executed in the

10 encrypted state. Decrypting is performed only in display and edit operations, and these are controlled by the copyright control program. In so doing, it is impossible to use the data beyond the permitted range. In this case, the copyright control program may be integrated with the data or may be encrypted.

15

Because the copyright control program is encrypted and the permit key decrypts the copyright control program, and because the copyright control program decrypts and encrypts the data, the data is encrypted twice.

a 20 In this case, if a ^{crypt}key unique to the data is added to the copyright control program for the purpose of encrypting the data, it is impossible to decrypt the data if the copyright control program is separated from the data.

a 25 In this copyright control program, even if the data is stored, copied or transferred within the permitted range of use, and if these operations are executed after the data and the copyright ^{control} program have been encrypted, it is impossible to use the data in an undesired manner.

30 If an operator uses a computer program inadequately and, as a result, the computer does not respond any more or computer operation is stopped, an error message is displayed so that the operator may know the cause.

Similarly, if a user of the database erroneously uses the data beyond the permitted range of the permit key, and, as a result, the computer does not respond or operation is stopped, the user cannot understand the cause. In this case, a copyright control message is displayed just as an error message is displayed by the copyright control program.

The display of the copyright control message as described above also fulfills the function of providing a warning if the user intentionally uses the data beyond the range of use permitted by the permit key.

In general, various programs are incorporated into read-only memory (ROM) inside the equipment which the user uses, or the programs are supplied from software. When the programs are incorporated into ROM, there is no possibility that the programs may be changed. However, the equipment ~~to be used~~ is limited to systems that contain the ROM. On the other hand, when the programs are supplied from software, there is no system limitation if the programs are transferred. However, there is a possibility that the programs may be altered. ^{Ins 06} ✓

The database is utilized by various users using various types of devices. Therefore, if the programs for controlling copyrights are supplied as software, it is necessary to cope with various types of devices. ~~Further, alteration of the programs must not be possible. Therefore, the copyright control program should be encrypted to prevent such trouble.~~ In this case, it is necessary to modify the program according to the device that the user uses. ^{Sub 07} ✓ ~~A program to~~ translate the copyright control program is provided in the communication software of the device which the user uses. The copyright control program can then be translated by the translation program so that it suits the device.

Even though the permit key for using the database may become more complicated due to encryption, a data size of several tens of bites is sufficient.

Therefore, the time required for transmitting the permit key is far shorter than one second. In other words, even when a payment-based public telephone line is used and other information is transmitted together with the permit key, the ^{Sub D₈} increase of cost is negligible.

D

5

Fig 3

Therefore, when transmitting the permit key as shown in Fig. 3B, utilizing surplus time, the copyright control program can be transmitted.

D

The copyright control program can be supplied together with the
10 permit key and also together with the data as shown in Fig. 3C.

D

In Fig. 3C

~~In this case~~, the copyright control program is supplied together with the data, and the entire data utilization process is placed under control of the copyright control program. For example, the data supplied in encrypted form
15 cannot be decrypted unless the copyright program supplied with it is used. If there is no such copyright control program, the data cannot be used. Thus,
D ~~the control of copyrights is reinforced.~~ Also, integration of the copyright control program with the data further reinforces copyright control.

20

Ins D₉

The following are some examples of the copyright control message:

"Need a display permit key."

"Need a storage permit key."

"Need a copying permit key."

25

"Need an edit permit key."

"Need a transfer permit key."

Some other examples are:

30

"Display unavailable."

"Storage unavailable."

"Copy unavailable."

"Edit unavailable."

"Transfer unavailable."

- 5 These copyright control messages are displayed alone as shown in Fig. 1A or in combination as shown in Fig. 1B.

Next, description will be given on supply of the copyright control message.

10

To display the copyright control message, the message must be stored in the memory of the device which the user uses. The memory in the device is classified as ROM and random-access memory (RAM).

- 15 The method of storing the messages in ROM is reliable, but there is a limitation to the device because the user must use the ROM wherein the copyright control messages are stored.

As for methods for storing messages in RAM, there is a method for
20 supplying messages together with the permit key, a method for supplying messages together with the copyright control program, and a method for supplying messages together with the data. When the permit key and the copyright control program are supplied at the same time, the copyright control message can also be supplied at the same time.

25

The copyright control message is not effective unless an adequate message is displayed. For this reason, the copyright control message cannot play its designed role if the message is changed in such a manner that no substantial content is displayed, or further, if its content is deleted such that
30 nothing is displayed. To prevent this trouble, the message is encrypted.

The display of the copyright control message is executed by the copyright control program. The modes of display are as follows. (1) When an operation is attempted with no adequate key available, a corresponding message is displayed. (2) All messages corresponding to operations available
5 for the current permit key are displayed, if an operation is attempted without an available permit key.

The copyright control message is supplied together with the permit key as shown in Fig. 3D, or together with the data as shown in Fig. 3E.

10

The copyright control message is transmitted by transmitting all messages or only the necessary messages required. In the former case, the quantity of information is relatively large, but security is high. In the latter case, the quantity of information is relatively small, but security is low.

15

It is desirable that the copyright control message be inseparable from the data, as in the case of the copyright control program. This may be facilitated by integrating the copyright control message with the copyright control program.

20

To display the copyright on printed matter, the name of the author and the date are used. The copyright of the database is displayed by entering information such as the name of the author and the date.

25

As described above, edit and up-load of edited data are included in the use of the data in the database. Specifically, the presence of secondary data, which is edited from the data, i.e. a work of authorship, is recognized. To ensure the copyright of the data in this context, it is necessary to store the information on original authorship and secondary authorship together with
D 30 the data. ^{When the data} ~~In case the data~~ is used in a manner other than for down-loading and display, copyright information including information on the operator, in

addition to the copyright information stored up to that moment, is stored together with the data as history.

In this case, only the person who controls the database can put the
5 original authorship into the database as primary data. All data handled by other than the person in charge of database control is considered secondary data. Control of the data history is therefore further reinforced.

When the copyright information is separated from data which is a
10 work of authorship, it becomes extremely difficult to recognize the copyright. Thus, it is necessary that the copyright information be inseparable from the data.

To prevent separation of the copyright information from the data, a
15 method for integrating the data with the copyright information or a method for making the data unusable without copyright information are described. These methods are similar to the methods described above for the copyright control program and the copyright control message.

20 First, description will be given for a method for integrating the data with the copyright information.

The data handled by computer comprises a file header indicating data name and size, and a file body, which comprises the main body of data.

25 Therefore, for integrating the data with the copyright information, there are methods that integrate the copyright information with the file header, that
D integrate the copyright information with the file body, and ^{that use other} ~~that take other~~
D ^{means for this purpose} ~~means for the purpose.~~

a 30 Among these methods, ^{for} the method that integrates the copyright
D information with file header ^{the} ~~is available even without a file header~~ if the ^{data is}
a

a
exp 8
A

character information is expressed with character code. Thus, ^{the method is} it is a simple method, but not very reliable. Also, because the capacity of the file header is not high, it is not sufficient if there is a large amount of copyright information.

5

Digital picture data and digital sound data are grouped together under a common group header. The copyright information can be integrated into this group header. However, there is a problem of header capacity similar to the case for the file header.

10

a For the method of integrating the copyright information with the file body, one way is to add copyright information for each ^{edited} edited piece of data. Another way is to add the copyright information all together.

a 15

To add the copyright information for each ^{edited} edited piece of data, the copyright information is added to each piece of data ^{edited} using a cut and paste procedure. ^{Sub D, which is edited by} This is not only complicated but disadvantageous in that the entire file data becomes too big.

20

If the picture data indicates the copyright of original authorship, it is easy to identify corresponding data. Thus, it is not always necessary to add the copyright information to each minimum unit of the edited data.

a

25

It is also possible to write the copyright information into the copyright ^{control} program. In this method, it is difficult to manipulate the copyright information if it is written into the copyright control program integrated with the data as already described.

30

If the data is a picture signal, it is necessary to have synchronization signal data in order to define scanning line, field and frame. This synchronization signal has high redundancy and is generally represented

with variable-length code. Thus, the copyright information can be mixed with the variable-length code. The number of scanning lines is 480 for VGA standards. By utilizing this method, a considerable quantity of information can be ~~mixed into it~~ ^{mixed into the picture signal}.

^{If} ~~In case~~ the picture data is an animated picture, it is possible to write a sufficient quantity of copyright information ^{using this method} ~~in this method~~. However, if the picture data is a still picture edited by a cut-and-paste procedure, there may not be enough space to add the copyright ~~control~~ information.

Fig. 2A and Fig. 2B represent structures for an analog television signal and a digital television signal. Fig. 2A represents an analog television signal, and Fig. 2B shows a digital television signal.

A signal containing other than picture data, such as the multiplex teletext signal in analog television, is inserted by utilizing the vertical retrace interval. The horizontal retrace interval is not utilized.

In contrast, in digital television, it is possible for a copyright control program or other multiplex teletext signal to be placed into horizontal scanning data or into vertical scanning data.

As a method for integrating the copyright information with data, one way is to write the copyright information into the data itself, and another is to write it into ^{the} control code.

With the data used in ^a computer, there is control code for controlling the communication system or computer system in addition to the data to be displayed on screen or used for some ^{operation} operation. This control code cannot be seen by the user. Therefore, if the copyright information is written into the

control code, the copyright information thus written does not cause trouble for the user.

It is also possible to enter ^{the copyright information} into the files of the computer using the technique of a computer virus without affecting the operation itself.

The copyright information may be supplied together with the permit key as shown in Fig. 3F ^{Fig. 3F or it may} or may be supplied together with data as shown in Fig. 3G.

Attention has been focused in recent years on digital signatures. ~~Using~~

a private key, which only the person concerned knows, and a public key, which other persons also know, a digital signature is prepared from the private key and from the data on the file size of the document. ^{data} If the document is changed, the change can be confirmed by the ^{data} private key, and the content of the document can be seen at any time by ^{private key} other persons using the public key. Thus, this scheme offers very high security.

The data in a computer can be changed without leaving any trace. Because of this, an author may not notice that his copyright is infringed, or a user may use the data without knowing that the content of the data has been changed, ~~and the author or user may suffer damages.~~ To prevent this, a digital signature is attached to the data, and damage to the copyright owner or the user can be avoided.

The permit key, copyright control program, copyright control message, and copyright information can be combined in any way as necessary to actualize the method for controlling database copyrights.

Also, it is possible to design in such a manner that only a part of the data of the copyright control program, the copyright control message or the

copyright information is supplied together with the permit key as shown in

a Sub D₃

Fig. 3H, 3I and 3J, and that the other part is supplied together with the data ^{to be utilized}

a 0

The part supplied with the permit key and the part supplied together with the data are combined. The functions of the complete permit key ^{may be} being served

5 after they have been combined together.

Thus, it is possible to give the function of the permit key to the copyright program and copyright control message, and higher security is ensured.

10